**IN THE UNITED STATES DISTRICT COURT**
**FOR THE NORTHERN DISTRICT OF GEORGIA**
**ATLANTA DIVISION**

| | |
|---|---|
| AMY DEROUIN, on behalf of themselves and all others similarly situated,<br><br>Plaintiff,<br><br>v.<br><br>NEXTGEN HEALTHCARE, INC.,<br><br>Defendant. | **Case No. _____**<br>**CLASS ACTION**<br>**JURY TRIAL DEMANDED** |

## CLASS ACTION COMPLAINT

Plaintiff Amy Derouin ("Plaintiff") bring this Class Action Complaint ("Complaint"), on behalf of herself and all others similarly situated, against NextGen Healthcare, Inc. ("NextGen" or "Defendant"), alleging as follows, based upon information and belief and investigation of counsel, except as to the allegations specifically pertaining to her, which are based on personal knowledge:

## NATURE OF THE CASE

1. Entities that provide services in the healthcare industry and handle patients' sensitive, personally identifying information ("PII" or "Private

Information") owe a duty to the individuals to whom that data relates. This duty arises because it is foreseeable that the exposure of patients' PII to unauthorized persons—especially hackers with nefarious intentions—will result in harm to the affected individuals, including, but not limited to, the invasion of their private health matters.

2. The harm resulting from a breach of private data manifests in a number of ways, including identity theft and financial fraud. The exposure of a person's PII through a data breach ensures that such person will be at a substantially increased and certainly impending risk of identity theft crimes compared to the rest of the population, potentially for the rest of their lives. Mitigating that risk—to the extent it is even possible to do so—requires individuals to devote significant time and money to closely monitor their credit, financial accounts, health records, and email accounts, and to take a number of additional prophylactic measures.

3. As a healthcare service provider, specifically a US-based business that provides electronic health records and practice management solutions to several healthcare organizations, NextGen knowingly obtains sensitive patient PII and has a resulting duty to securely maintain such information in confidence.

4. NextGen's Notice of Privacy Policy acknowledges that "[w]e use reasonably and appropriate security measures designed to protect the personal information we obtain from unauthorized alteration, loss, disclosure, or use, including technological, physical and administrative controls…."[1] The Privacy Policy delineates the specific ways in which NextGen discloses information "[w]e may also disclose information as we believe necessary…."[2]

5. As discussed in more detail below, NextGen breached its duty to protect the sensitive PII entrusted to it, and failed to abide by its own Privacy Policies. As such, Plaintiff brings this Class action on behalf of herself and the over 1 million other patients whose PII was accessed and exposed to unauthorized third parties during a data breach of Defendant's system on or about March 29, 2023, which NextGen announced on or about April 28, 2023 (the "Data Breach").[3]

6. Indeed, NextGen did not inform Plaintiff of the Data Breach until April 28, 2023, twenty-eight days after NextGen first discovered the Data Breach.[4]

---

[1] *Privacy Policy*, NEXTGEN (May 9, 2023), https://www.nextgen.com/privacy-policy.

[2] *Id.*

[3] *NextGen Healthcare Cyber Attack Exposes Patient Data for Nearly 17 Days,* THE CYBER EXPRESS (May 2, 2023), https://thecyberexpress.com/nextgen-healthcare-cyber-attack-data-exposed/ (Defendant alerted on March 30, 2023).

[4] *Id.*

7. Based on the public statements of NextGen to date, a wide variety of PII was implicated in the breach, including but not limited to, patients' names, dates of birth, Social Security numbers and addresses.[5]

8. As a direct and proximate result of NextGen's inadequate data security, and its breach of its duty to handle PII with reasonable care, Plaintiff's PII has been accessed by hackers, posted on the dark web, and exposed to an untold number of unauthorized individuals.

9. Plaintiff is now at a significantly increased and certainly impending risk of fraud, identity theft, misappropriation of health insurance benefits, intrusion of her health privacy, and similar forms of criminal mischief, risk which may last for the rest of her life. Consequently, Plaintiff must devote substantially more time, money, and energy to protect herself, to the extent possible, from these crimes.

10. Plaintiff, on behalf of herself and others similarly situated, bring claims for negligence, negligence *per se*, breach of fiduciary duty, breach of confidences, breach of an implied contract, unjust enrichment, and declaratory judgment, seeking actual and putative damages, with attorneys' fees, costs, and expenses, and appropriate injunctive and declaratory relief.

---

[5] *NextGen Healthcare, Inc. Reports Data Breach Affecting Thousands of Individuals' Social Security Numbers,* JDSUPRA (May 1, 2023) https://www.jdsupra.com/legalnews/nextgen-healthcare-inc-reports-data-7912620/

11. To recover from NextGen for her sustained, ongoing, and future harms, Plaintiff seeks damages in an amount to be determined at trial, declaratory judgment, and injunctive relief requiring Defendant to: 1) disclose, expeditiously, the full nature of the Data Breach and the types of PII accessed, obtained, or exposed by the hackers; 2) implement improved data security practices to reasonably guard against future breaches of PII possessed by Defendant; and 3) provide, at its own expense, all impacted victims with lifetime identity theft protection services.

## PARTIES

### Plaintiff

12. Plaintiff is an adult who at all relevant times is a citizen of Westfield, Massachusetts who resides in Hampden County.

13. Plaintiff Derouin's PII was stored and handled by NextGen. Plaintiff Derouin has regular visits with her Obstetrician/Gynecologist, as recently as February 2023, as well as with her primary care Physician, as recently in 2022. On or around May 1, 2023, Plaintiff Derouin was notified by Nextgen via letter dated April 28, 2023 of the Data Breach and of the impact to her PII.

14. As a result of Defendant's conduct, Plaintiff suffered actual damages including, without limitation, time related to monitoring her financial accounts for

fraudulent activity, facing an increased and imminent risk of fraud and identity theft, the lost value of her personal information, and other economic and non-economic harm. Plaintiff and Class members will now be forced to expend additional time, efforts, and potentially expenses to review her credit reports, monitor her financial accounts, and monitor for fraud or identify theft – particularly since the compromised information may include Social Security numbers.

**Defendant**

15. Defendant NextGen Healthcare, Inc. is a business incorporated in Delaware, with its headquarters located at 3525 Piedmont Rd., NE Building 6, Suite 700 Atlanta, GA.

16. Defendant NextGen provides software and related support to ambulatory medical providers, including practice management, revenue cycle management, patient experience, value-based care, analytics & reporting, and data platforms.[6]

[6] *NextGen Healthcare, Inc. Reports Data Breach Affecting Thousands of Individuals' Social Security Numbers,* JDSUPRA (May 1, 2023) https://www.jdsupra.com/legalnews/nextgen-healthcare-inc-reports-data-7912620/.

## JURISDICTION AND VENUE

17. This Court has subject matter jurisdiction over this matter pursuant to 28 U.S.C. § 1332(d). The amount in controversy in this Class action exceeds $5,000,000, exclusive of interest and costs, and there are numerous Class members who are citizens of states other than Defendant's state of citizenship.

18. This Court has personal jurisdiction over the parties in this case. Defendant NextGen conducts business in this District and is a citizen of this District by virtue of having its principal place of business located in this District.

19. Venue is proper in this District under 28 U.S.C. §1391(b) because NextGen and/or its parents or affiliates are headquartered in this District and a substantial part of the events or omissions giving rise to Plaintiff's claims occurred in this District.

## FACTUAL BACKGROUND

### A. NextGen and the Services it Provides.

20. NexGen is a healthcare organization that produces electronic health record (EHR) software and practice management systems for over 100,000 providers, hospitals and clinics across all 50 states.[7]

[7] NextGen Healthcare, Inc., *Form 10K* (March 31, 2022) https://investor.nextgen.com/static-files/c1cd4035-fc46-48ac-8471-8a2170231a3f.

21. While administering services, NextGen receives and handles PII, which includes, *inter alia*, patients' full name, address, date of birth, Social Security Number, driver's license or state ID number, financial account and payment card information, medical information, and health insurance information.

22. In order to receive services from NextGen, Plaintiff is required to entrust their highly sensitive PII to Defendant. Plaintiff entrusted this information to NextGen with the reasonable expectation and mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

23. Indeed, NextGen contains a comprehensive Privacy Policy that acknowledges its obligations to keep Plaintiff's PII confidential and secure from unauthorized access.[8] The policy indicates that NextGen will only share this sensitive information with certain third parties who have entered into agreements with it "[w]e enter into contracts with our third party vendors that limit how they may use and disclosure of the information to the purposes for which we disclosed it to them."[9]

[8] *Privacy Policy*, NEXTGEN (May 9, 2023), https://www.nextgen.com/privacy-policy.

[9] *Id.*

24. By obtaining, collecting, and storing Plaintiff's PII, NextGen assumed legal and equitable duties and knew or should have known that Defendant was responsible for protecting Plaintiff's PII from unauthorized disclosure.

25. And, upon information and belief, Defendant funds its data security measures entirely from its general revenue, including payments made by or on behalf of Plaintiff and the Class members.

## B. NextGen Knew the Risks of Storing Valuable PII and the Foreseeable Harm to its Patients.

26. At all relevant times, NextGen knew it was storing sensitive PII and that, as a result, its systems would be an attractive target for cybercriminals.

27. NextGen also knew that a breach of its systems, and exposure of the information stored therein, would result in the increased risk of identity theft and fraud against the individuals whose PII was compromised, as well as intrusion into their highly private health information.

28. These risks are not theoretical. The healthcare industry has become a prime target for threat actors: "High demand for patient information and often-outdated systems are among the nine reasons healthcare is now the biggest target for online attacks."[10]

[10] *The healthcare industry is at risk*, SWIVELSECURE https://swivelsecure.com/solutions/

29. As further evidence of this heightened risk, Nextgen had already experienced a ransomware attack earlier in 2023.[11]

30. "Hospitals store an incredible amount of patient data. Confidential data that's worth a lot of money to hackers who can sell it on easily – making the industry a growing target."[12]

31. The healthcare sector suffered about 337 breaches in the first half of 2022 alone, according to Fortified Health Security's mid-year report released in July 2022. The percentage of healthcare breaches attributed to malicious activity rose more than 5 percentage points in the first six months of 2022 to account for nearly 80 percent of all reported incidents.[13]

---

healthcare/healthcare-is-the-biggest-target-for-cyberattacks/ (last visited Apr. 17, 2023).

[11] *NextGen Healthcare says hackers accessed personal data of more than 1 million patients*, https://techcrunch.com/2023/05/08/nextgen-healthcare-data-breach/amp/ (last visited May 11, 2023).

[12] *Id.*

[13] Jill McKeon, *Health Sector Suffered 337 Healthcare Data Breaches in First Half of Year*, CYBERSECURITY NEWS (July 19, 2022), https://healthitsecurity.com/news/health-sector-suffered-337-healthcare-data-breaches-in-first-half-of-year.

32. Further, a 2022 report released by IBM Security stated that for 12 consecutive years the healthcare industry has had the highest average cost of a data breach and as of 2022 healthcare data breach costs have hit a new record high.[14]

33. Indeed, cyberattacks against the healthcare industry have been common for over the past ten years with the Federal Bureau of Investigation ("FBI") warning as early as 2011 that cybercriminals were "advancing their abilities to attack a system remotely" and "[o]nce a system is compromised, cyber criminals will use their accesses to obtain PII." The FBI further warned that that "the increasing sophistication of cyber criminals will no doubt lead to an escalation in cybercrime."[15]

34. Cyberattacks have become so notorious that the FBI and U.S. Secret Service have issued a warning to potential targets so they are aware of, and prepared for, a potential attack. As one report explained, "[e]ntities like smaller municipalities and hospitals are attractive to ransomware criminals… because they

[14] *Cost of a Data Breach Report 2022*, IBM SECURITY, https://www.ibm.com/downloads/cas/3R8N1DZJ (last visited Apr. 17, 2023).

[15] Gordon M. Snow, *Statement before the House Financial Services Committee, Subcommittee on Financial Institutions and Consumer Credit*, FBI (Sept. 14, 2011), https://archives.fbi.gov/archives/news/testimony/cyber-security-threats-to-the-financial-sector.

often have lesser IT defenses and a high incentive to regain access to their data quickly.[16]

35. In tandem with the increase in data breaches, the rate of identity theft complaints has also increased over the past few years. For instance, in 2017, 2.9 million people reported some form of identity fraud compared to 5.7 million people in 2021.[17]

36. The type and breadth of data compromised in the Data Breach makes the information particularly valuable to thieves and leaves Defendant's patients especially vulnerable to identity theft, tax fraud, medical fraud, credit and bank fraud, and more.

37. PII is a valuable property right.[18] The value of PII as a commodity is

---

[16] Ben Kochman, *FBI, Secret Service Warn of Targeted Ransomware*, LAW360 (Nov. 18, 2019), https://www.law360.com/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware.

[17] *Insurance Information Institute, Facts + Statistics: Identity theft and cybercrime*, Insurance Information Institute, https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime#Identity%20Theft%20And%20Fraud%20Reports,%202015-2019%20 (last visited Apr. 17, 2023).

[18] *See* Marc Van Lieshout, *The Value of Personal Data*, 457 IFIP ADVANCES IN INFORMATION & COMMUNICATION TECHNOLOGY 26 (May 2015), https://www.researchgate.net/publication/283668023_The_Value_of_Personal_Data ("The value of [personal] information is well understood by marketers who try to collect as much data about personal conducts and preferences as possible . . . . ").

measurable.[19] "Firms are now able to attain significant market valuations by employing business models predicated on the successful use of personal data within the existing legal and regulatory frameworks."[20] American companies are estimated to have spent over $19 billion on acquiring personal data of consumers in 2018.[21] It is so valuable to identity thieves that once PII has been disclosed, criminals often trade it on the "cyber black-market," or the "dark web," for many years.

38. As a result of their real value and the recent large-scale data breaches, identity thieves and cyber criminals have openly posted credit card numbers, Social Security numbers, PII, and other sensitive information directly on various Internet websites, making the information publicly available. This information from various breaches, including the information exposed in the Data Breach, can

[19] Robert Lowes, *Stolen EHR [Electronic Health Record] Charts Sell for $50 Each on Black Market*, MEDSCAPE (Apr. 28, 2014), http://www.medscape.com/viewarticle. /824192.

[20] *Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value*, OECD 4 (Apr. 2, 2013), https://www.oecd-ilibrary.org/science-and-technology/exploring-the-economics-of-personal-data_5k486qtxldmq-en.

[21] *U.S. Firms to Spend Nearly $19.2 Billion on Third-Party Audience Data and Data-Use Solutions in 2018, Up 17.5% from 2017*, INTERACTIVE ADVERTISING BUREAU (Dec. 5, 2018), https://www.iab.com/news/2018-state-of-data-report/.

be aggregated, and becomes more valuable to thieves and more damaging to victims.

39. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches: "[I]n some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the [Dark] Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm."[22]

40. Even if stolen PII does not include financial or payment card account information, that does not mean there has been no harm, or that the breach does not cause a substantial risk of identity theft. Freshly stolen information can be used with success against victims in specifically targeted efforts to commit identity theft known as social engineering or spear phishing. In these forms of attack, the criminal uses the previously obtained PII about the individual, such as name, address, email address, and affiliations, to gain trust and increase the likelihood that a victim will be deceived into providing the criminal with additional information.

[22] United States Government Accountability Office, Report to Congressional Requesters, Personal Information, June 2007: https://www.gao.gov/new.items/d07737.pdf (last visited Apr. 17, 2023).

41. Consumers place a high value on the privacy of that data. Researchers shed light on how much consumers value their data privacy—and the amount is considerable. Indeed, studies confirm that "when privacy information is made more salient and accessible, some consumers are willing to pay a premium to purchase from privacy protective websites." [23]

42. Given these facts, any company that transacts business with a consumer and then compromises the privacy of consumers' PII has thus deprived that consumer of the full monetary value of the consumer's transaction with the company.

43. Based on the value of its patients' PII to cybercriminals and cybercriminals' propensity to target healthcare providers, NextGen certainly knew the foreseeable risk of failing to implement adequate cybersecurity measures.

## C. NextGen Breached its Duty to Protect its Patients' PII.

44. On April 28, 2023, NextGen announced that it experienced a security incident disrupting access to its systems.[24]

---

[23] Janice Y. Tsai et al., *The Effect of Online Privacy Information on Purchasing Behavior*, *An Experimental Study*, 22(2) Information Systems Research 254 (June 2011), https://www.guanotronic.com/~serge/papers/weis07.pdf.

[24] *NextGen Healthcare, Inc. Reports Data Breach Affecting Thousands of Individuals' Social Security Numbers*, *supra* n. 5.

45. According to NextGen, once they were made aware of the cyberattack, they "began to review the affected files to determine what information was compromised and which consumers were impacted."[25]

46. By April 28, 2023, the investigation confirmed that data containing PII may have been accessed or acquired by an unauthorized third party.[26]

47. After the investigation revealed that PII may have been accessed or acquired by an unauthorized third party, NextGen conducted a review process to confirm what it already knew—that PII of current and former patients had been compromised.[27]

48. As noted above, the patient PII compromised in the Data Breach includes patient names, dates of birth, Social Security Numbers, driver's license or state ID numbers, financial account and/or payment information, medical information, and health insurance information.[28]

49. According to a JD Supra report, on April 28, 2023 NextGen filed a notice of the Data Breach with the Attorney Generals of Montana, Texas and Maine alerting that a "data security incident impacting the company's computer

[25] *Id.*

[26] *Id.*

[27] *Id.*

[28] *Id.*

network resulted in confidential consumer information being made accessible to an unauthorized party."[29]

50. On or about the same date that NextGen reported the Data Breach and provided a notice to Plaintiff indicating that their PII may have been compromised or accessed during the Data Breach.

51. Like Plaintiff, other potential Class members received similar notices informing them that their PII was exposed in the Data Breach.

52. All in all, approximately 1,049,375 of individuals with information stored on NextGen's system had their PII breached.[30]

53. The Data Breach occurred as a direct result of Defendant's failure to implement and follow basic security procedures in order to protect its patients' PII.

## D. FTC Guidelines Prohibit NextGen from Engaging in Unfair or Deceptive Acts or Practices.

54. NextGen is prohibited by the Federal Trade Commission Act, 15 U.S.C. § 45 ("FTC Act") from engaging in "unfair or deceptive acts or practices in or affecting commerce." The Federal Trade Commission ("FTC") has concluded that a company's failure to maintain reasonable and appropriate data security for

[29] *NextGen Healthcare Cyber Attack Exposes Patient Data for Nearly 17 Days, supra* note 3.

[30] *Id.*

consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act.

55. The FTC has promulgated numerous guides for businesses that highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[31]

56. The FTC provided cybersecurity guidelines for businesses, advising that businesses should protect personal customer information, properly dispose of personal information that is no longer needed, encrypt information stored on networks, understand their network's vulnerabilities, and implement policies to correct any security problems.[32]

57. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to private data; require complex passwords to be used on networks; use industry-tested methods

[31] *Start with Security – A Guide for Business*, United States Federal Trade Comm'n (2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.

[32] *Protecting Personal Information: A Guide for Business*, United States Federal Trade Comm'n, https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personalinformation.pdf.

for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.[33]

58. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the FTC Act. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

59. NextGen failed to properly implement basic data security practices. NextGen's failure to employ reasonable and appropriate measures to protect against unauthorized access to patient PII constitutes an unfair act of practice prohibited by Section 5 of the FTC Act.

60. NextGen was at all times fully aware of its obligations to protect the PII of patients because of its position as a healthcare provider, which gave it direct access to reams of patient PII. Defendant was also aware of the significant repercussions that would result from its failure to do so.

[33] *Id.*

## E. Cyberattacks and Data Breaches Cause Disruption and Put Consumers at an Increased Risk of Fraud and Identity Theft.

61. Cyberattacks and data breaches at healthcare companies like NextGen are especially problematic because they can negatively impact the overall daily lives of individuals affected by the attack.

62. Researchers have found that among healthcare service providers that experience a data security incident, the death rate among patients increased in the months and years after the attack.[34]

63. Researchers have further found that at healthcare service providers that experienced a data security incident, the incident was associated with deterioration in timeliness and patient outcomes, generally.[35]

64. The United States Government Accountability Office released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage

[34] *See* Nsikan Akpan, *Ransomware and Data Breaches Linked to Uptick in Fatal Heart Attacks*, PBS (Oct. 24, 2019), https://www.pbs.org/newshour/science/ransomware-and-other-data-breaches-linked-to-uptick-in-fatal-heart-attacks.

[35] *See* Sung J. Choi et al., *Data Breach Remediation Efforts and Their Implications for Hospital Quality*, 54 HEALTH SERVICES RESEARCH 971, 971-980 (2019), https://onlinelibrary.wiley.com/doi/full/10.1111/1475-6773.13203.

to their good name and credit record."[36]

65. That is because any victim of a data breach is exposed to serious ramifications regardless of the nature of the data. Indeed, the reason criminals steal personally identifiable information is to monetize it. They do this by selling the spoils of their cyberattacks on the black market to identity thieves who desire to extort and harass victims, and to take over victims' identities in order to engage in illegal financial transactions under the victims' names. Because a person's identity is akin to a puzzle, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity, or otherwise harass or track the victim. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails.

[36] *See* U.S. Gov. Accounting Office, GAO-07-737, Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown (2007), https://www.gao.gov/new.items/d07737.pdf.

66. Theft of PII is serious. The FTC warns consumers that identity thieves use PII to exhaust financial accounts, receive medical treatment, open new utility accounts, and incur charges and credit in a person's name.

67. The FTC recommends that identity theft victims take several steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (and consider an extended fraud alert that lasts for 7 years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing freezes on their credit, and correcting their credit reports.[37]

68. Identity thieves use stolen personal information such as Social Security numbers for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud. According to Experian, one of the largest credit reporting companies in the world, "[t]he research shows that personal information is valuable to identity thieves, and if they can get access to it, they will use it" to among other things: open a new credit card or loan, change a billing address so the victim no longer receives bills, open new utilities, obtain a mobile

[37] *See IdentityTheft.gov*, Federal Trade Commission, https://www.identitytheft.gov/Steps (last accessed Feb. 24, 2023).

phone, open a bank account and write bad checks, use a debit card number to withdraw funds, obtain a new driver's license or ID, and/or use the victim's information in the event of arrest or court action.

69. Identity thieves can also use the victim's name and Social Security number to obtain government benefits; or file a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's Social Security number, and/or rent a house or receive medical services in the victim's name.

70. Moreover, theft of PII is also gravely serious because PII is an extremely valuable property right.[38]

71. Drug manufacturers, medical device manufacturers, pharmacies, hospitals, and other healthcare service providers often purchase PII on the black market for the purpose of target-marketing their products and services to the physical maladies of the data breach victims themselves.

72. Each year, identity theft causes tens of billions of dollars of losses to victims in the United States. For example, with the PII stolen in the Data Breach,

[38] *See, e.g.*, John T. Soma, et al., *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets*, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

which includes Social Security numbers, identity thieves can open financial accounts, commit medical fraud, apply for credit, file fraudulent tax returns, commit crimes, create false driver's licenses and other forms of identification and sell them to other criminals or undocumented immigrants, steal government benefits, give breach victims' names to police during arrests, and many other harmful forms of identity theft. These criminal activities have and will result in devastating financial and personal losses to Plaintiff.

73. As discussed above, PII is such a valuable commodity to identity thieves, and once the information has been compromised, criminals often trade the information on the "cyber black-market" for years.

74. Social security numbers are particularly sensitive pieces of personal information. As the Consumer Federation of America explains:

> **Social Security number:** *This is the most dangerous type of personal information in the hands of identity thieves* because it can open the gate to serious fraud, from obtaining credit in your name to impersonating you to get medical services, government benefits, your tax refund, employment—even using your identity in bankruptcy and other legal matters. It's hard to change your Social Security number and it's not a good idea because it is connected to your lift in so many ways. [39]

[39] *See, e.g.*, Christine DiGangi, *5 Ways an Identity Thief Can Use Your Social Security Number* (Nov. 2, 2017), https://blog.credit.com/2017/11/5-things-an-identity-thief-can-do-with-your-social-security-number-108597/ (emphasis added).

75. For instance, with a stolen Social Security number, which is only one subset of the PII compromised in the Data Breach, someone can open financial accounts, get medical care, file fraudulent tax returns, commit crimes, and steal benefits.[40]

76. The Social Security Administration has warned that identity thieves can use an individual's Social Security number to apply for additional credit lines.[41] Such fraud may go undetected until debt collection calls commence months, or even years, later. Stolen Social Security numbers also make it possible for thieves to file fraudulent tax returns, file for unemployment benefits, or apply for a job using a false identity.[42] Each of these fraudulent activities is difficult to detect. An individual may not know that his or her Social Security number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected because one was already filed on their behalf.

77. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. Even then, a new Social

[40] *Id.*

[41] *Id.*

[42] *Id.* at 4.

Security number may not be effective, as "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[43]

78. This was a financially motivated Data Breach, as the only reason the cybercriminals go through the trouble of running a targeted cyberattack against companies like NextGen is to get information that they can monetize by selling on the black market for use in the kinds of criminal activity described herein. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "[c]ompared to credit card information, personally identifiable information and Social Security Numbers are worth more than 10x on the black market."

79. Indeed, a Social Security number, date of birth, and full name can sell for $60 to $80 on the digital black market.[44] "[I]f there is reason to believe that

[43] Brian Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft.

[44] Michael Kan, *Here's How Much Your Identity Goes for on the Dark Web*, (Nov. 15, 2017), https://www.pcmag.com/news/heres-how-much-your-identity-goes-for-on-the-dark-web.

your personal information has been stolen, you should assume that it can end up for sale on the dark web."[45]

80. These risks are both certainly impending and substantial. As the FTC has reported, if hackers get access to PII, they *will use it.*[46]

81. There may also be a time lag between when sensitive personal information is stolen, when it is used, and when a person discovers it has been used. Fraud and identity theft resulting from the Data Breach may go undetected until debt collection calls commence months, or even years, later. As with income tax returns, an individual may not know that his or her Social Security Number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud.

82. For example, on average it takes approximately three months for consumers to discover their identity has been stolen and used, and it takes some individuals up to three years to learn that information.[47]

---

[45] *Dark Web Monitoring: What You Should Know*, Consumer Federation of America (Mar. 19, 2019), https://consumerfed.org/consumer_info/dark-web-monitoring-what-you-should-know/.

[46] *Id.*

[47] John W. Coffey, *Difficulties in Determining Data Breach Impacts*, 17 JOURNAL OF SYSTEMICS, CYBERNETICS AND INFORMATICS 9 (2019), http://www.iiisci.org/journal/pdv/sci/pdfs/IP069LL19.pdf.

83. Cybercriminals can post stolen PII on the cyber black-market for years following a data breach, thereby making such information publicly available.

84. Approximately 21% of victims do not realize their identity has been compromised until more than two years after it has happened. [48] This gives thieves ample time to seek multiple treatments under the victim's name. Forty percent of consumers found out they were a victim of medical identity theft only when they received collection letters from creditors for expenses that were incurred in their names.[49]

85. Identity theft victims must spend countless hours and large amounts of money repairing the impact to their credit as well as protecting themselves in the future.[50]

86. It is within this context that Plaintiff must now live with the knowledge that their PII is forever in cyberspace and was taken by people willing

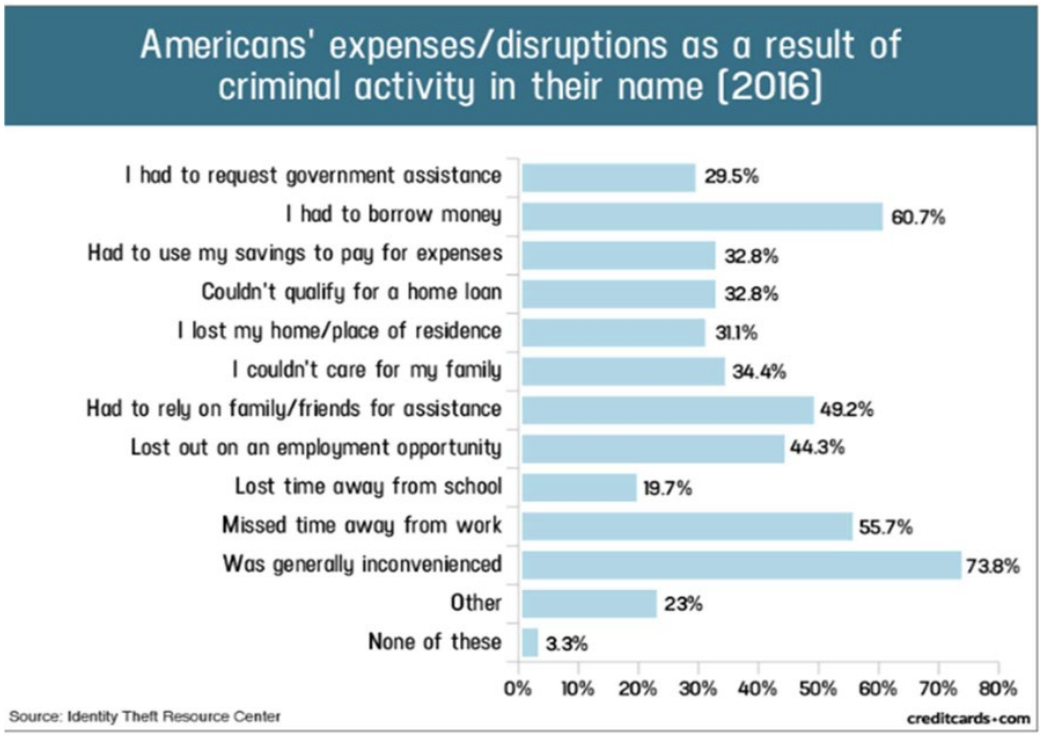
[48] *See* Medical ID Theft Checklist, https://www.identityforce.com/blog/medical-id-theft-checklist-2 (last visited Apr. 17, 2023).

[49] *The Potential Damages and Consequences of Medical Identify Theft and Healthcare Data Breaches ("Potential Damages")*, EXPERIAN, https://www.experian.com/assets/data-breach/white-papers/consequences-medical-id-theft-healthcare.pdf (last visited Apr. 17, 2023).

[50] *Guide for Assisting Identity Theft Victims*, FED. TRADE COMM'N, 4 (Sept. 2013), http://www.consumer.ftc.gov/articles/pdf-0119-guide-assisting-id-theft-victims.pdf.

to use the information for any number of improper purposes and scams, including making the information available for sale on the black market.

87. A study by the Identity Theft Resource Center shows the multitude of harms caused by fraudulent use of personal and financial information.




88. Victims of the Data Breach, like Plaintiff, must spend many hours and large amounts of money protecting themselves from the current and future negative impacts to their privacy and credit because of the Data Breach.[51]

89. As a direct and proximate result of the Data Breach, Plaintiff has had their PII exposed, have suffered harm as a result, and have been placed at an

[51] *Id.*

imminent, immediate, and continuing increased risk of harm from fraud and identity theft. Plaintiff must now take the time and effort (and spend the money) to mitigate the actual and potential impact of the Data Breach on their everyday lives, including purchasing identity theft and credit monitoring services every year for the rest of their lives, placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions and healthcare providers, closing or modifying financial accounts, and closely reviewing and monitoring bank accounts, credit reports, and health insurance account information for unauthorized activity for years to come.

90. Moreover, Plaintiff and Class members have an interest in ensuring that their PII, which remains in the possession of NextGen, is protected from further public disclosure by the implementation of better employee training and industry standard and statutorily compliant security measures and safeguards. NextGen has shown itself to be wholly incapable of protecting Plaintiff's PII.

91. Plaintiff and Class members also have an interest in ensuring that their personal information that was provided to NextGen is removed from NextGen's unencrypted files.

92. NextGen acknowledged, in its letter to Plaintiff, that, in response to the Data Breach, that NextGen has taken "measures to contain the incident."[52]

93. Because of the value of its collected and stored data, the medical industry has experienced disproportionally higher numbers of data theft events than other industries. For this reason, NextGen knew or should have known about these dangers and strengthened its data security accordingly. NextGen was put on notice of the substantial and foreseeable risk of harm from a data breach, yet it failed to properly prepare for that risk.

**F. Plaintiff Suffered Damages.**

94. NextGen received Plaintiff's and class members' PII in connection with providing certain medical services and treatment to them. In requesting and maintaining Plaintiff's PII for business purposes, NextGen expressly and impliedly promised, and undertook a duty, to act reasonably in its handling of Plaintiff's and Class members' PII. NextGen did not, however, take proper care of Plaintiff's and Class members' PII, leading to its exposure to and exfiltration by cybercriminals as a direct result of NextGen's inadequate security measures.

95. For the reasons mentioned above, NextGen's conduct, which allowed the Data Breach to occur, caused Plaintiff and Class members significant injuries

[52] *See* NextGen, Data Breach Letter (April 28, 2023).

and harm in several ways. Plaintiff and Class members must immediately devote time, energy, and money to: 1) closely monitor their medical statements, bills, records, and credit and financial accounts; 2) change login and password information on any sensitive account even more frequently than they already do; 3) more carefully screen and scrutinize phone calls, emails, and other communications to ensure that they are not being targeted in a social engineering or spear phishing attack; and 4) search for suitable identity theft protection and credit monitoring services, and pay to procure them. Plaintiff and Class members have taken or will be forced to take these measures in order to mitigate their potential damages as a result of the Data Breach.

96. Once PII is exposed, there is little that can be done to ensure that the exposed information has been fully recovered or obtained against future misuse. For this reason, Plaintiff and Class members will need to maintain these heightened measures for years, and possibly their entire lives as a result of Defendant's conduct.

97. Further, the value of Plaintiff's and Class members' PII has been diminished by its exposure in the Data Breach. Plaintiff and Class members did not receive the full benefit of their bargain when paying for medical services, and instead received services that were of a diminished value to those described in their

agreements with NextGen for the benefit and protection of Plaintiff and their respective PII. Plaintiff and Class members were damaged in an amount at least equal to the difference in the value between the services they thought they paid for (which would have included adequate data security protection) and the services they actually received.

98. Plaintiff and Class members would not have obtained medical services from NextGen, or paid the amount they did to receive such, had they known that NextGen would negligently fail to adequately protect their PII. Indeed, Plaintiff and Class members paid for medical services with the expectation that NextGen would keep their PII secure and inaccessible from unauthorized parties. Plaintiff and class members would not have obtained services from NextGen had they known that Defendant failed to properly train its employees, lacked safety controls over its computer network, and did not have proper data security practices to safeguard their PII from criminal theft and misuse.

99. As a result of Defendant's failures, Plaintiff and Class members are also at substantial and certainly impending increased risk of suffering identity theft and fraud or misuse of their PII.

100. Further, because Defendant delayed in notifying Plaintiff about the Data Breach for nearly five months, Plaintiff was unable to take affirmative steps

during that time period to attempt to mitigate any harm or take prophylactic steps to protect against injury.

101. From a recent study, 28% of consumers affected by a data breach become victims of identity fraud—this is a significant increase from a 2012 study that found only 9.5% of those affected by a breach would be subject to identity fraud. Without a data breach, the likelihood of identify fraud is only about 3%.[53]

102. "Actors buying and selling PII from healthcare institutions and providers in underground marketplaces is very common and will almost certainly remain so due to this data's utility in a wide variety of malicious activity ranging from identity theft and financial fraud to crafting of bespoke phishing lures."[54]

103. Plaintiff is also at a continued risk because their information remains in NextGen's computer systems, which have already been shown to be susceptible to compromise and attack and is subject to further attack so long as NextGen fails to undertake the necessary and appropriate security and training measures to protect its patients' PII.

---

[53] Stu Sjouwerman, *28 Percent of Data Breaches Lead to Fraud*, KNOWBE4, https://blog.knowbe4.com/bid/252486/28-percent-of-data-breaches-lead-to-fraud (last visited Apr. 17, 2023).

[54] David, *supra* note 67.

104. In addition, Plaintiff and Class members have suffered emotional distress as a result of the Data Breach, the increased risk of identity theft and financial fraud, and the unauthorized exposure of their private medical information to strangers.

## CLASS ALLEGATIONS

105. Plaintiff brings all counts, as set forth below, individually and as a Class action, pursuant to the provisions of the Fed. R. Civ. P. 23, on behalf of a Class defined as:

> All persons in the United States who had their Private Information submitted to Defendant or Defendant's affiliates and/or whose Private Information was compromised as a result of the data breach(es) discovered by NextGen on or about March 30, 2023, including all who received a Notice of the Data Breach (the "Class").

106. Excluded from the Class are Defendant, its subsidiaries and affiliates, officers and directors, any entity in which Defendant has a controlling interest, the legal representative, heirs, successors, or assigns of any such excluded party, the judicial officer(s) to whom this action is assigned, and the members of their immediate families.

107. This proposed Class definition is based on the information available to Plaintiff at this time. Plaintiff may modify the Class definition in an amended pleading or when they move for Class certification, as necessary to account for any

newly learned or changed facts as the situation develops and discovery gets underway.

108. **Numerosity – Fed. R. Civ. P. 23(a)(1)**: Plaintiff is informed and believe, and thereon allege, that there are at minimum, thousands of members of the Class described above. The exact size of the Class and the identities of the individual members are identifiable through NextGen's records, including but not limited to the files implicated in the Data Breach, but based on public information, the Class includes approximately 1.1 million individuals.

109. **Commonality – Fed. R. Civ. P. 23(a)(2):** This action involves questions of law and fact common to the Class. Such common questions include, but are not limited to:

a. Whether NextGen failed to timely notify Plaintiff of the Data Breach;

b. Whether NextGen had a duty to protect the PII of Plaintiff and Class members;

c. Whether NextGen was negligent in collecting and storing Plaintiff's and Class members' PII, and breached its duties thereby;

d. Whether Defendant breached its fiduciary duty to Plaintiff and the Class;

e. Whether NextGen breached its duty of confidence to Plaintiff and the Class;

f. Whether NextGen violated its own Privacy Practices;

g. Whether NextGen entered a contract implied in fact with Plaintiff and the Class;

h. Whether NextGen breached that contract by failing to adequately safeguard Plaintiff's and Class members' PII;

i. Whether NextGen was unjustly enriched;

j. Whether Plaintiff and Class members are entitled to damages as a result of NextGen's wrongful conduct; and

k. Whether Plaintiff and Class members are entitled to restitution as a result of NextGen's wrongful conduct.

110. **Typicality – Fed. R. Civ. P. 23(a)(3)**: Plaintiff's claims are typical of the claims of the members of the Class. The claims of the Plaintiff and members of the Class are based on the same legal theories and arise from the same unlawful and willful conduct. Plaintiff and members of the Class all had information stored in NextGen's System, each having their PII exposed and/or accessed by an unauthorized third party.

111. **Adequacy of Representation – Fed. R. Civ. P. 23(a)(3)**: Plaintiff is an adequate representative of the Class because her interests do not conflict with the interests of the other Class members Plaintiff seeks to represent; Plaintiff has retained counsel competent and experienced in complex Class action litigation; Plaintiff intends to prosecute this action vigorously; and Plaintiff's counsel has adequate financial means to vigorously pursue this action and ensure the interests of the Class will not be harmed. Furthermore, the interests of the Class members will be fairly and adequately protected and represented by Plaintiff and Plaintiff's counsel.

112. **Injunctive Relief, Fed. R. Civ. P. 23(b)(2):** Defendant has acted and/or refused to act on grounds that apply generally to the Class therefore making injunctive and/or declarative relief appropriate with respect to the Class under 23(b)(2).

113. **Superiority, Fed. R. Civ. P. 23(b)(3):** A Class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a Class action, most Class members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution

of separate actions by individual Class members would create a risk of inconsistent or varying adjudications with respect to individual Class members, which would establish incompatible standards of conduct for NextGen. In contrast, the conduct of this action as a Class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class member.

114. NextGen has acted on grounds that apply generally to the Class as a whole, so that Class certification, injunctive relief, and corresponding declaratory relief are appropriate on a Class-wide basis.

115. Likewise, particular issues are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether NextGen failed to timely and adequately notify the public of the Data Breach;

b. Whether NextGen owed a legal duty to Plaintiff and the Class to exercise due care in collecting, storing, and safeguarding their PII;

c. Whether NextGen's security measures to protect its data systems were reasonable in light of best practices recommended by data security experts;

d. Whether NextGen's failure to institute adequate protective security measures amounted to negligence;

e. Whether NextGen failed to take commercially reasonable steps to safeguard consumer PII; and

f. Whether adherence to FTC data security recommendations, and measures recommended by data security experts would have reasonably prevented the Data Breach.

116. Finally, all members of the proposed Class are readily ascertainable. NextGen has access to Class members' names and addresses affected by the Data Breach. Class members have already been preliminarily identified and sent notice of the Data Breach by NextGen.

**FIRST CAUSE OF ACTION**
**NEGLIGENCE**
**(Plaintiff on behalf of the Class)**

117. Plaintiff restates and realleges the preceding allegations above as if fully alleged herein.

118. Plaintiff brings this claim individually and on behalf of the Class.

119. Defendant owed a duty to Plaintiff and Class members to exercise reasonable care in safeguarding and protecting their PII in its possession, custody, and control.

120. Defendant's duty to use reasonable care arose from several sources, including but not limited to those described below.

121. Defendant had a common law duty to prevent foreseeable harm to others. This duty existed because Plaintiff and Class members were the foreseeable and probable victims of any inadequate security practices on the part of the Defendant. By collecting and storing valuable PII that is routinely targeted by criminals for unauthorized access, Defendant was obligated to act with reasonable care to protect against these foreseeable threats.

122. Defendant's duty also arose from Defendant's position as a healthcare vendor. Defendant holds itself out as a trusted provider of services for the healthcare industry, and thereby assumes a duty to reasonably protect patients' information.

123. Defendant breached the duties owed to Plaintiff and Class members and thus was negligent. As a result of a successful attack directed towards Defendant that compromised Plaintiff's and Class members' PII, Defendant

breached its duties through some combination of the following errors and omissions that allowed the data compromise to occur:

(a) mismanaging its system and failing to identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that resulted in the unauthorized access and compromise of PII; (b) mishandling its data security by failing to assess the sufficiency of its safeguards in place to control these risks; (c) failing to design and implement information safeguards to control these risks; (d) failing to adequately test and monitor the effectiveness of the safeguards' key controls, systems, and procedures; (e) failing to evaluate and adjust its information security program in light of the circumstances alleged herein; (f) failing to detect the breach at the time it began or within a reasonable time thereafter; (g) failing to follow its own privacy policies and practices published to its patients; and (h) failing to adequately train and supervise employees and third party vendors with access or credentials to systems and databases containing sensitive PII.

124. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiff and Class members, their PII would not have been compromised.

125. As a direct and proximate result of Defendant's negligence, Plaintiff and Class members have suffered injuries, including, but not limited to:

a. Theft of their PII;

b. Costs associated with the detection and prevention of identity theft and unauthorized use of their PII;

c. Costs associated with purchasing credit monitoring and identity theft protection services;

d. Lowered credit scores resulting from credit inquiries following fraudulent activities;

e. Costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Data Breach – including finding fraudulent charges, cancelling and reissuing cards, enrolling in credit monitoring and identity theft protection services, freezing and unfreezing accounts, and imposing withdrawal and purchase limits on compromised accounts;

f. The imminent and certainly impending injury flowing from the increased risk of potential fraud and identity theft posed by their PII being placed in the hands of criminals;

g. Damages to and diminution in value of their PII entrusted, directly or indirectly, to Defendant with the mutual understanding that Defendant

would safeguard Plaintiff's and Class members' data against theft and not allow access and misuse of their data by others;

h. Continued risk of exposure to hackers and thieves of their PII, which remains in Defendant's possession and is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiff's and Class members' data; and

i. Emotional distress from the unauthorized disclosure of PII to strangers who likely have nefarious intentions and now have prime opportunities to commit identity theft, fraud, and other types of attacks on Plaintiff and Class members.

126. As a direct and proximate result of Defendant's negligence, Plaintiff and Class members are entitled to damages, including compensatory, punitive, and/or nominal damages, in an amount to be proven at trial.

**SECOND CAUSE OF ACTION**
**NEGLIGENCE PER SE**
**(Plaintiff on behalf of the Class)**

127. Plaintiff restates and realleges the preceding allegations above as if fully alleged herein.

128. Plaintiff brings this claim individually and on behalf of the Class.

129. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice by entities such as Defendant for failing to use reasonable measures to protect PII. Various FTC publications and orders also form the basis of Defendant's duty.

130. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with the industry standards. Defendant's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored and the foreseeable consequences of a data breach involving PII of its patients.

131. Plaintiff and members of the Class are consumers within the Class of persons Section 5 of the FTC Act was intended to protect.

132. Defendant's violation of Section 5 of the FTC Act constitutes negligence *per se*.

133. The harm that has occurred as a result of Defendant's conduct is the type of harm that the FTC Act and Part 2 was intended to guard against.

134. As a direct and proximate result of Defendant's negligence, Plaintiff has been injured as described herein, and are entitled to damages, including compensatory, punitive, and nominal damages, in an amount to be proven at trial.

**THIRD CAUSE OF ACTION**
**BREACH OF FIDUCIARY DUTY**
**(Plaintiff on behalf of the Class)**

135. Plaintiff restates and realleges the preceding allegations above as if fully alleged herein.

136. Plaintiff and Class members have an interest, both equitable and legal, in the PII about them that was conveyed to, collected by, and maintained by Defendant and that was ultimately accessed or compromised in the Data Breach.

137. As a provider of electronic health record software, and recipient of patients' PII, Defendant has a fiduciary relationship to its patients, including Plaintiff and the Class members.

138. Because of that fiduciary relationship, Defendant was provided with and stored private and valuable PII related to Plaintiff and the Class. Plaintiff and the Class were entitled to expect their information would remain confidential while in Defendant's possession.

139. Defendant owed a fiduciary duty under common law to Plaintiff and Class members to exercise the utmost care in obtaining, retaining, securing, safeguarding, deleting, and protecting their PII in Defendant's possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons.

140. As a result of the parties' fiduciary relationship, Defendant had an obligation to maintain the confidentiality of the information within Plaintiff's and the Class members' medical records.

141. Defendant's patients, including Plaintiff and Class members, have a privacy interest in personal medical matters, and NextGen had a fiduciary duty not to disclose medical data concerning its patients.

142. As a result of the parties' relationship, Defendant had possession and knowledge of confidential PII of Plaintiff and Class members, information not generally known.

143. Plaintiff and Class members did not consent to nor authorize Defendant to release or disclose their PII to unknown criminal actors.

144. Defendant breached its fiduciary duties owed to Plaintiff and Class members by, among other things:

a. mismanaging its system and failing to identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that resulted in the unauthorized access and compromise of PII;

b. mishandling its data security by failing to assess the sufficiency of its safeguards in place to control these risks;

c. failing to design and implement information safeguards to control these risks;

d. failing to adequately test and monitor the effectiveness of the safeguards' key controls, systems, and procedures;

e. failing to evaluate and adjust its information security program in light of the circumstances alleged herein;

f. failing to detect the breach at the time it began or within a reasonable time thereafter;

g. failing to follow its own privacy policies and practices published to its patients; and

h. failing to adequately train and supervise employees and third-party vendors with access or credentials to systems and databases containing sensitive PII.

145. But for Defendant's wrongful breach of its fiduciary duties owed to Plaintiff and Class members, their PII would not have been compromised.

146. As a direct and proximate result of Defendant's negligence, Plaintiff and Class members have suffered injuries, including:

a. Theft of their PII;

b. Costs associated with the detection and prevention of identity theft and unauthorized use of their PII;

c. Costs associated with purchasing credit monitoring and identity theft protection services;

d. Lowered credit scores resulting from credit inquiries following fraudulent activities;

e. Costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Data Breach – including finding fraudulent charges, cancelling and reissuing cards, enrolling in credit monitoring and identity theft protection services, freezing and unfreezing accounts, and imposing withdrawal and purchase limits on compromised accounts;

f. The imminent and certainly impending injury flowing from the increased risk of potential fraud and identity theft posed by their PII being placed in the hands of criminals;

g. Damages to and diminution in value of their PII entrusted, directly or indirectly, to Defendant with the mutual understanding that Defendant

would safeguard Plaintiff's data against theft and not allow access and misuse of their data by others;

h. Continued risk of exposure to hackers and thieves of their PII, which remains in Defendant's possession and is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiff's data; and

i. Emotional distress from the unauthorized disclosure of PII to strangers who likely have nefarious intentions and now have prime opportunities to commit identity theft, fraud, and other types of attacks on Plaintiff.

147. As a direct and proximate result of Defendant's breach of its fiduciary duties, Plaintiff and Class members are entitled to damages, including compensatory, punitive, and/or nominal damages, in an amount to be proven at trial.

## FOURTH CAUSE OF ACTION
## BREACH OF CONFIDENCE
## (Plaintiff on behalf of the Class)

148. Plaintiff restates and realleges the preceding allegations above as if fully alleged herein.

149. Plaintiff and Class Member have an interest, both equitable and legal, in the PII about them that was conveyed to, collected by, and maintained by Defendant and that was ultimately accessed or compromised in the Data Breach.

150. As a healthcare provider, Defendant has a special relationship to its patients, like Plaintiff and the Class members.

151. Plaintiff provided Defendant with their personal and confidential PII under both the express and/or implied agreement of Defendant to limit the use and disclosure of such PII.

152. Defendant owed a duty to Plaintiff to exercise the utmost care in obtaining, retaining, securing, safeguarding, deleting, and protecting their PII in its possession from being compromised, lost, stolen, accessed by, misused by, or disclosed to unauthorized persons.

153. As a result of the parties' relationship, Defendant had possession and knowledge of confidential PII and confidential medical records of Plaintiff.

154. Plaintiff's PII is not generally known to the public and is confidential by nature.

155. Plaintiff did not consent to nor authorize Defendant to release or disclose their PII to an unknown criminal actor.

156. Defendant breached the duties of confidence it owed to Plaintiff when Plaintiff's PII was disclosed to unknown criminal hackers.

157. Defendant breached its duties of confidence by failing to safeguard Plaintiff's PII, including by, among other things: (a) mismanaging its system and failing to identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that resulted in the unauthorized access and compromise of PII; (b) mishandling its data security by failing to assess the sufficiency of its safeguards in place to control these risks; (c) failing to design and implement information safeguards to control these risks; (d) failing to adequately test and monitor the effectiveness of the safeguards' key controls, systems, and procedures; (e) failing to evaluate and adjust its information security program in light of the circumstances alleged herein; (f) failing to detect the breach at the time it began or within a reasonable time thereafter; (g) failing to follow its on privacy policies and practices published to its patients; (h) storing PII and medical records/information in an unencrypted and vulnerable manner, allowing its disclosure to hackers; and (i) making an unauthorized and unjustified disclosure and release of Plaintiff's PII and medical records/information to a criminal third party.

158. But for Defendant's wrongful breach of its duty of confidences owed to Plaintiff, their privacy, confidences, and PII would not have been compromised.

159. As a direct and proximate result of Defendant's breach of Plaintiff's confidences, Plaintiff has suffered injuries, including:

a. The erosion of the essential and confidential relationship between Defendant – as a health care services provider – and Plaintiff as a patient;

b. Theft of their PII;

c. Costs associated with the detection and prevention of identity theft and unauthorized use of their PII ;

d. Costs associated with purchasing credit monitoring and identity theft protection services;

e. Lowered credit scores resulting from credit inquiries following fraudulent activities;

f. Costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the NextGen Data Breach – including finding fraudulent charges, cancelling and reissuing cards, enrolling in credit monitoring and identity theft protection services,

freezing and unfreezing accounts, and imposing withdrawal and purchase limits on compromised accounts;

g. The imminent and certainly impending injury flowing from the increased risk of potential fraud and identity theft posed by their PII being placed in the hands of criminals;

h. Damages to and diminution in value of their PII entrusted, directly or indirectly, to Defendant with the mutual understanding that Defendant would safeguard Plaintiff's data against theft and not allow access and misuse of their data by others;

i. Continued risk of exposure to hackers and thieves of their PII, which remains in Defendant's possession and is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiff's data; and

j. Loss of personal time spent carefully reviewing statements from health insurers and providers to check for charges for services not received, as directed to do by Defendant.

160. Additionally, Defendant received payments from Plaintiff for services with the understanding that Defendant would uphold its responsibilities to maintain the confidences of Plaintiff's private medical information.

161. Defendant breached the confidence of Plaintiff when it made an unauthorized release and disclosure of their confidential medical information and, accordingly, it would be inequitable for Defendant to retain the benefit at Plaintiff's expense.

162. As a direct and proximate result of Defendant's breach of its duty of confidences, Plaintiff is entitled to damages, including compensatory, punitive, and/or nominal damages, and/or disgorgement or restitution, in an amount to be proven at trial.

## FIFTH CAUSE OF ACTION
## INTRUSION UPON SECLUSION/INVASION OF PRIVACY
## (Plaintiff on behalf of the Class)

163. Plaintiff restates and realleges the preceding allegations above as if fully alleged herein.

164. Plaintiff had a reasonable expectation of privacy in the PII Defendant mishandled.

165. Defendant's conduct as alleged above intruded upon Plaintiff's and Class members' seclusion under common law.

166. By intentionally failing to keep Plaintiff's PII safe, and by intentionally misusing and/or disclosing said information to unauthorized parties

for unauthorized use, Defendant intentionally invaded Plaintiff's and Class members' privacy by:

a. Intentionally and substantially intruding into Plaintiff's and Class members' private affairs in a manner that identifies Plaintiff and Class members and that would be highly offensive and objectionable to an ordinary person;

b. Intentionally publicizing private facts about Plaintiff and Class members, which is highly offensive and objectionable to an ordinary person; and

c. Intentionally causing anguish or suffering to Plaintiff and Class members.

167. Defendant knew that an ordinary person in Plaintiff's or Class members' position would consider Defendant's intentional actions highly offensive and objectionable.

168. Defendant invaded Plaintiff's and Class members' right to privacy and intruded into Plaintiff's and Class members' private affairs by intentionally misusing and/or disclosing their PII without their informed, voluntary, affirmative, and clear consent.

169. Defendant intentionally concealed from and delayed reporting to Plaintiff and Class members a security incident that misused and/or disclosed their PII without their informed, voluntary, affirmative, and clear consent.

170. The conduct described above was at or directed at Plaintiff and the Class members.

171. As a proximate result of such intentional misuse and disclosures, Plaintiff's and Class members' reasonable expectations of privacy in their PII was unduly frustrated and thwarted. Defendant's conduct amounted to a substantial and serious invasion of Plaintiff's and Class members' protected privacy interests causing anguish and suffering such that an ordinary person would consider Defendant's intentional actions or inaction highly offensive and objectionable.

172. In failing to protect Plaintiff's and Class members' PII, and in intentionally misusing and/or disclosing their PII, Defendant acted with intentional malice and oppression and in conscious disregard of Plaintiff's and Class members' rights to have such information kept confidential and private. Plaintiff, therefore, seeks an award of damages on behalf of herself and the Class.

173. As a direct and proximate result of NextGen's conduct, Plaintiff and Class members are entitled to damages, including compensatory, punitive, and/or nominal damages, in an amount to be proven at trial.

**SIXTH CAUSE OF ACTION**
**BREACH OF IMPLIED CONTRACT**
**(Plaintiff on behalf of the Class)**

174. Plaintiff restates and realleges the preceding allegations above as if fully alleged herein.

175. Plaintiff brings this claim individually and on behalf of the Class.

176. When Plaintiff and members of the Class provided their PII to NextGen in exchange for healthcare services, they entered into implied contracts with Defendant, under which NextGen agreed to take reasonable steps to protect Plaintiff's and Class members' PII, comply with it statutory and common law duties to protect Plaintiff's PII, and to timely notify them in the event of a data breach.

177. NextGen solicited and invited Plaintiff and Class members to provide their PII as part of Defendant's provision of healthcare services. Plaintiff accepted Defendant's offers and provided their PII to Defendant.

178. When entering into implied contracts, Plaintiff and Class members reasonably believed and expected that Defendant's data security practices complied with its statutory and common law duties to adequately protect Plaintiff's PII and to timely notify them in the event of a data breach.

179. NextGen's implied promise to safeguard patient PII is evidenced by, *e.g.*, the representations in Defendant's Notice of Privacy Practices set forth above.

180. Plaintiff and Class members paid money to Defendant in order to receive healthcare services. Plaintiff and Class members reasonably believed and expected that Defendant would use part of those funds to obtain adequate data security. NextGen failed to do so.

181. Plaintiff would not have provided their PII to NextGen had they known that Defendant would not safeguard their PII, as promised, or provide timely notice of a data breach.

182. Plaintiff and Class members fully performed their obligations under their implied contracts with NextGen.

183. NextGen breached its implied contracts with Plaintiff and Class members by failing to safeguard Plaintiff's and Class members' PII and by failing to provide them with timely and accurate notice of the Data Breach.

184. The losses and damages Plaintiff sustained, include, but are not limited to:

a. Theft of her PII;

b. Costs associated with purchasing credit monitoring and identity theft protection services;

c. Costs associated with the detection and prevention of identity theft and unauthorized use of their PII;

d. Lowered credit scores resulting from credit inquiries following fraudulent activities;

e. Costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Data Breach – including finding fraudulent charges, cancelling and reissuing cards, enrolling in credit monitoring and identity theft protection services, freezing and unfreezing accounts, and imposing withdrawal and purchase limits on compromised accounts;

f. The imminent and certainly impending injury flowing from the increased risk of potential fraud and identity theft posed by their PII being placed in the hands of criminals;

g. Damages to and diminution in value of their PII entrusted, directly or indirectly, to Defendant with the mutual understanding that Defendant would safeguard Plaintiff's and Class members' data against theft and not allow access and misuse of their data by others;

h. Continued risk of exposure to hackers and thieves of their PII, which remains in Defendant's possession and is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiff's and Class members' data; and

i. Emotional distress from the unauthorized disclosure of PII to strangers who likely have nefarious intentions and now have prime opportunities to commit identity theft, fraud, and other types of attacks on Plaintiff and Class members.

185. As a direct and proximate result of NextGen's breach of contract, Plaintiff and Class members are entitled to damages, including compensatory, punitive, and/or nominal damages, in an amount to be proven at trial.

## SEVENTH CAUSE OF ACTION
## UNJUST ENRICHMENT
## (Plaintiff on behalf of the Class)

186. Plaintiff restates and realleges the preceding allegations above as if fully alleged herein.

187. Plaintiff brings this claim individually and on behalf of the Class in the alternative to Plaintiff's Implied Contract claim.

188. Upon information and belief, Defendant funds its data security measures entirely from its general revenue, including payments made by or on behalf of Plaintiff and the Class members.

189. As such, a portion of the payments made by or on behalf of Plaintiff and the Class members is to be used to provide a reasonable level of data security, and the amount of the portion of each payment made that is allocated to data security is known to Defendant.

190. Plaintiff and Class members conferred a monetary benefit on Defendant. Specifically, they purchased healthcare services from Defendant and/or its agents and in so doing provided Defendant with their PII. In exchange, Plaintiff and Class members should have received from Defendant the goods and services that were the subject of the transaction and have their PII protected with adequate data security.

191. Defendant knew that Plaintiff and Class members conferred a benefit which Defendant accepted. Defendant profited from these transactions and used the PII of Plaintiff and Class members for business purposes.

192. In particular, Defendant enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiff's and Class members' PII. Instead of providing a reasonable level of security that

would have prevented the Data Breach, Defendant instead calculated to increase its own profits at the expense of Plaintiff and Class members by utilizing cheaper, ineffective security measures. Plaintiff and Class members, on the other hand, suffered as a direct and proximate result of Defendant's decision to prioritize its own profits over the requisite security.

193. Under the principles of equity and good conscience, Defendant should not be permitted to retain the money belonging to Plaintiff and Class members, because Defendant failed to implement appropriate data management and security measures that are mandated by its common law and statutory duties.

194. Defendant failed to secure Plaintiff and Class members' PII and, therefore, did not provide full compensation for the benefit Plaintiff and Class members provided.

195. Defendant acquired the PII through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

196. If Plaintiff and Class members knew that Defendant had not reasonably secured their PII, they would not have agreed to provide their PII to Defendant.

197. Plaintiff and Class members have no adequate remedy at law.

198. As a direct and proximate result of Defendant's conduct, Plaintiff and Class members have suffered injuries, including, but not limited to:

a. Theft of their PII;

b. Costs associated with purchasing credit monitoring and identity theft protection services;

c. Costs associated with the detection and prevention of identity theft and unauthorized use of their PII;

d. Lowered credit scores resulting from credit inquiries following fraudulent activities;

e. Costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Data Breach – including finding fraudulent charges, cancelling and reissuing cards, enrolling in credit monitoring and identity theft protection services, freezing and unfreezing accounts, and imposing withdrawal and purchase limits on compromised accounts;

f. The imminent and certainly impending injury flowing from the increased risk of potential fraud and identity theft posed by their PII being placed in the hands of criminals;

g. Damages to and diminution in value of their PII entrusted, directly or indirectly, to Defendant with the mutual understanding that Defendant would safeguard Plaintiff's and Class members' data against theft and not allow access and misuse of their data by others;

h. Continued risk of exposure to hackers and thieves of their PII, which remains in Defendant's possession and is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiff's and Class members' data; and

i. Emotional distress from the unauthorized disclosure of PII to strangers who likely have nefarious intentions and now have prime opportunities to commit identity theft, fraud, and other types of attacks on Plaintiff and Class members.

199. As a direct and proximate result of Defendant's conduct, Plaintiff and Class members have suffered and will continue to suffer other forms of injury and/or harm.

200. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class members, proceeds that they unjustly received from them. In the alternative, Defendant should be

compelled to refund the amounts that Plaintiff and Class members overpaid for Defendant's services.

**EIGHTH CAUSE OF ACTION**
**DECLARATORY JUDGMENT**
**(Plaintiff on behalf of the Class)**

201. Plaintiff restates and realleges the preceding allegations the paragraphs above as if fully alleged herein.

202. Plaintiff brings this claim individually and on behalf of the Class.

203. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq*., this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and granting further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal statutes described in this Complaint.

204. An actual controversy has arisen in the wake of the Data Breach regarding Defendant's present and prospective common law and other duties to reasonably safeguard Plaintiff's and Class members' PII, and whether Defendant is currently maintaining data security measures adequate to protect Plaintiff and Class members from future data breaches that compromise their PII. Plaintiff and the Class remain at imminent risk that additional compromises of their PII will occur in the future.

205. The Court should also issue prospective injunctive relief requiring Defendant to employ adequate security practices consistent with law and industry standards to protect consumers' PII.

206. Defendant still possesses the PII of Plaintiff and the Class.

207. Defendant has made no announcement that it has changed its data storage or security practices relating to the storage of Plaintiff's and Class members' PII.

208. To Plaintiff's knowledge, Defendant has made no announcement or notification that it has remedied the vulnerabilities and negligent data security practices that led to the Data Breach.

209. If an injunction is not issued, Plaintiff and the Class will suffer irreparable injury and lack an adequate legal remedy in the event of another data breach at NextGen. The risk of another such breach is real, immediate, and substantial.

210. The hardship to Plaintiff and Class members if an injunction does not issue exceeds the hardship to Defendant if an injunction is issued. Among other things, if another data breach occurs at NextGen, Plaintiff and Class members will likely continue to be subjected to a heightened, substantial, imminent risk of fraud, identify theft, and other harms described herein. On the other hand, the cost to

Defendant of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Defendant has a pre-existing legal obligation to employ such measures.

211. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach at NextGen, thus eliminating the additional injuries that would result to Plaintiff and Class members, along with other consumers whose PII would be further compromised.

212. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring that NextGen implement and maintain reasonable security measures, including but not limited to the following:

a. Engaging third-party security auditors/penetration testers, as well as internal security personnel, to conduct testing that includes simulated attacks, penetration tests, and audits on NextGen's systems on a periodic basis, and ordering NextGen to promptly correct any problems or issues detected by such third-party security auditors;

b. Engaging third-party security auditors and internal personnel to run automated security monitoring;

c. Auditing, testing, and training its security personnel regarding any new or modified procedures;

d. Purging, deleting, and destroying PII not necessary for its provisions of services in a reasonably secure manner;

e. Conducting regular database scans and security checks; and

f. Routinely and continually conducting internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach.

**PRAYER FOR RELIEF**

WHEREFORE, Plaintiff, on behalf of herself and all others similarly situated, prays for relief as follows:

a. For an Order certifying this action as a Class action and appointing Plaintiff as Class Representative and their counsel as Class Counsel;

b. For equitable relief enjoining NextGen from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and Class members' PII, and from refusing to issue prompt, complete and accurate disclosures to Plaintiff and Class members;

c. For equitable relief compelling NextGen to utilize appropriate methods and policies with respect to consumer data collection, storage, and safety,

and to disclose with specificity the type of Personal Information compromised during the Data Breach;

d. For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of NextGen's wrongful conduct;

e. Ordering NextGen to pay for not less than three years of credit monitoring services for Plaintiff and the Class;

f. For an award of actual damages, compensatory damages, statutory damages, and statutory penalties, in an amount to be determined, as allowable by law;

g. For an award of punitive damages, as allowable by law;

h. For an award of attorneys' fees and costs, and any other expense, including expert witness fees;

i. Pre- and post-judgment interest on any amounts awarded; and,

j. Such other and further relief as this court may deem just and proper.

**JURY TRIAL DEMANDED**

A jury trial is demanded by Plaintiff on all claims so triable.

Dated: May 11, 2023

Respectfully submitted,

*/s/ G. Franklin Lemond, Jr.*
G. Franklin Lemond, Jr., Esq.
**WEBB, KLASE & LEMOND, LLC**
1900 The Exchange, SE, Suite 480
Atlanta, Georgia 30339
T: (770) 444-9594
flemond@webbllc.com

Jonathan Shub*
Benjamin F. Johns*
Samantha Holbrook*
**SHUB & JOHNS LLC**
Four Tower Bridge
200 Barr Harbor Drive, Suite 400
Conshohocken, PA 19428
T: (610) 477-8380
bjohns@shublawyers.com
jshub@shublawyers.com
sholbrook@shublawyers.com

E. Powell Miller*
Emily E. Hughes
Gregory A. Mitchell
**THE MILLER LAW FIRM, P.C.**
950 W. University Dr., Suite 300
Rochester, MI 48307
Tel: (248) 841-2200
epm@millerlawpc.com
eeh@millerlawpc.com
gam@millerlawpc.com

* *pro hac vice* forthcoming

*Attorneys for Plaintiff and the Putative Class*